Digital Forensics - CSE 574

Class: T/R - 5:30 - 7:17pm Math and Science Center 364
Jan 04, 2018 - April 17, 2018

Course Instructor:
Gautam B. Singh, PhD, JD
x2129, singh@oakland.edu

Book
Bill Nelson, Amelia Phillips, Christopher Steuart, Guide to Computer Forensics and Investigations, Fifth Edition. Cengage Learning, 2016, ISBN-13: 978-1-285-06003-3.

Final Examination: April 19, 2017, 7 – 10 PM.

Catalog: This course provides a general overview of the fundamentals of computer forensics, the role of a cyber forensics specialist, computer forensic evidence and introduction of real world problems in collecting and processing digital evidence.

Major Topics:

- Digital Forensic Science and Laws related to Computer Forensics
- Computer Crimes and Cyber Forensics
- Seizure of Digital Evidence and Crime Scene Analysis
- Forensics Tools for Recovery of Data from Computers, Smartphones and Disks
- Cloud Forensics

Labs
There will be 2 case assignments. Each of the teams will be working as "forensic experts" to try and ascertain as much evidence as needed for developing either a civil or criminal case against an individual or group of individuals.

For Case I: Group designated as the group seeking to **admit** the evidence, and a group that will seek to deem it **inadmissible** by critically questioning the other teams' evidence gathering process.

For Case II: Each group will create a disk with 5 items of forensically relevant data in a disk image and supply this disk image to a different group. Also each group will look for evidence in disk image supplied by another group and discover evidence.

Types of forensics data: Deleted Files, Hidden Data, Password Protected Files - Password Cracking, Steganographic Messages, Deleted Emails, Web Browser Cache Data, Web Search Terms, Social Media Posts, Network File Transfers, Etc.

Grade Distribution	
Laboratory Assignments	20%
In-class Assignments and Participation/Short Presentations	10%
Case I - Fourth Amendment Issues	10%
Case II - Forensics Analysis - Report and Presentations	20%
Quizzes	20%
Final Exam (Take Home)	20%

Schedule - Each Topic Approximately 2 weeks

Introduction to Cybercrime, Electronic evidence	Chapter(s) - 1	1. Examples of electronic evidence 2. What are some of the challenges in admitting electronic evidence
Issue in collecting electronic evidence	Chapter(s) - 2, 3	1. What is the fourth amendment 2. What are the issues in handling electronic evidence 3. CASE 1 - Team and Assignment
Processing Crime Scene	Chapter(s) - 4	1. Identifying Evidence 2. Chain of Custody / Hash Codes 3. Rules of Evidence **4. CASE 1 PRESENTATIONS**
Working with Windows and Linux	Chapter(s) - 5, 7	1. Windows FAT, NTFS, Encryption 2. Registry, MFT - File Structure 3. Linux - Tools, Linux Commands 4. Live CD - Linux
Graphics Files, File Carving	Chapter(s) - 8	1. CASE 2 - Team and Assignment 2. Steganography 3. File Headers and Trailers
Network Forensics, Email Forensics	Chapter(s) - 10, 11	1. Tools used in Network Forensics 2. Web Browsing, Network Access 3. Final Examination Assigned - Take Home
Mobile Device Forensics, Cloud Forensics	Chapter(s) - 12, 13	**1. CASE 2 PRESENTATIONS** 2. Discussion - Final Exam
FINAL EXAMINATION		Final